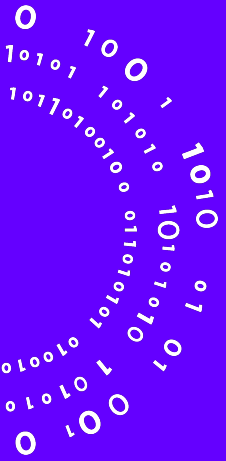


Cryptography Research Centre

Syndrome Decoding Estimator

by Andre Esser and Emanuele Bellini

Cryptography Research Center, Technology Innovation Institute, UAE

TII Technology Innovation Institute

Motivation

Cryptography Research Centre

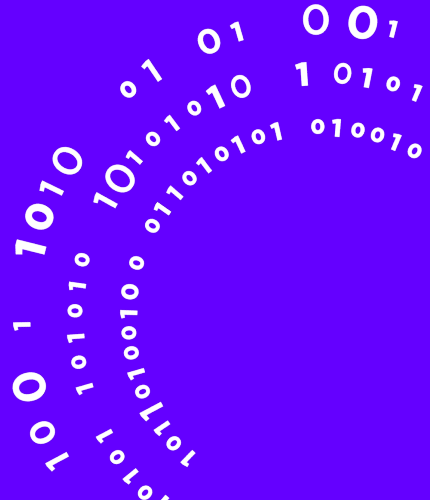
- NIST PQC approaching selection
- Exact security level of proposed parameters?
- Classic McEliece, BIKE, HQC

Goal: Precise security estimates under different metrics

Results

- Unify Information Set Decoding (ISD) landscape
- Syndrome Decoding Estimator
- Precise Security Estimates

Syndrome Decoding



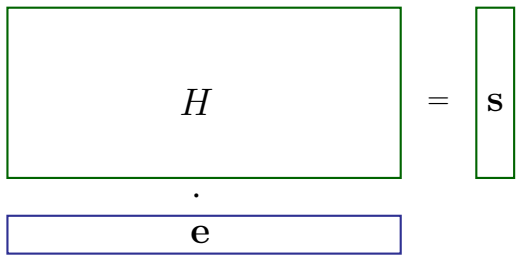
Syndrome Decoding

Cryptography Research Centre

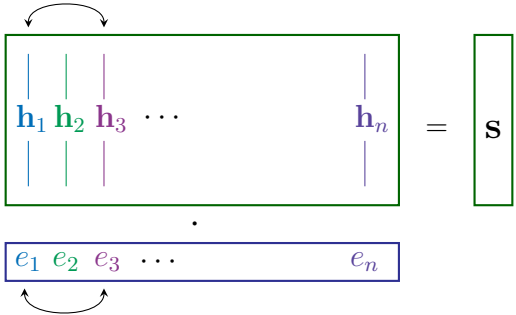
Definition (Syndrome Decoding)

given : parity-check matrix $H \in \mathbb{F}_2^{(n-k)\times n}$, syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$, error-weight $\omega \in \mathbb{N}$

find : error-vector $\mathbf{e} \in \mathbb{F}_2^n$ with: $H\mathbf{e}^\top = \mathbf{s}$ and $\mathrm{wt}(\mathbf{e}) = \omega$

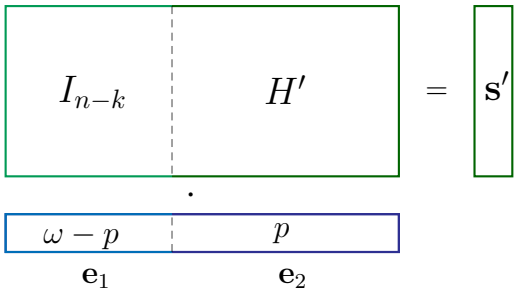


Permuting an Instance



$$(HP)(P^{-1}\mathbf{e}) = \mathbf{s}$$

Nearest Neighbor



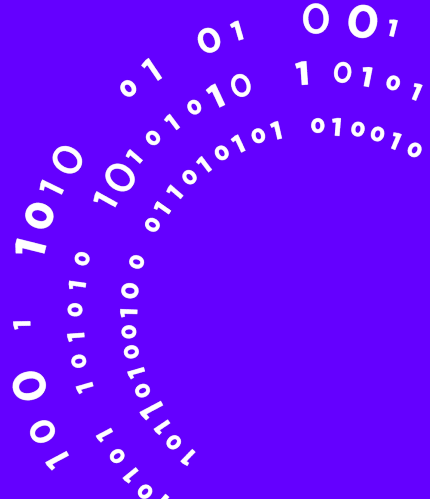
$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$

ISD:

1. Permute
2. Gauss
3. Solve

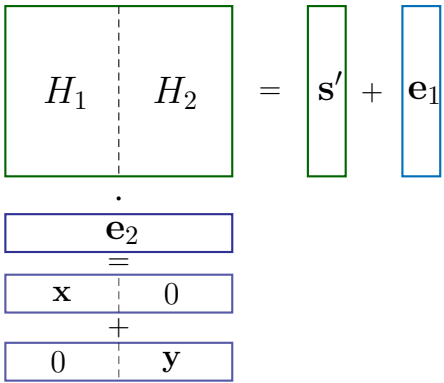
$$H'\mathbf{e}_2 \approx_{\mathbf{e}_1} \mathbf{s}'$$

Information Set Decoding (ISD)



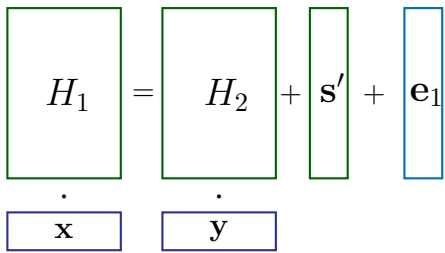
Stern and Dumer

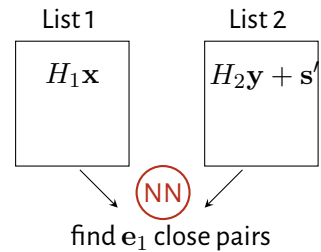
$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$



Stern and Dumer

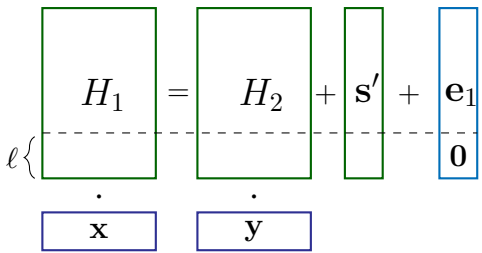
$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$



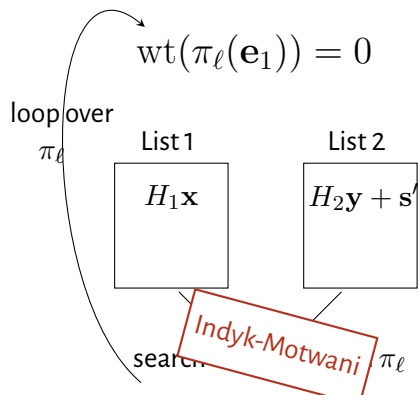


Stern and Dumer

$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$

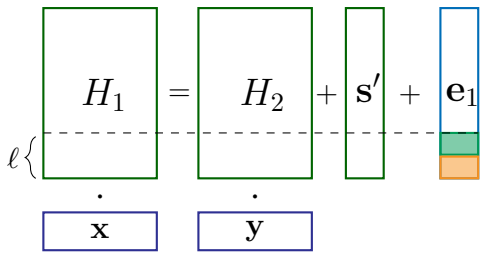


Stern's Algorithm



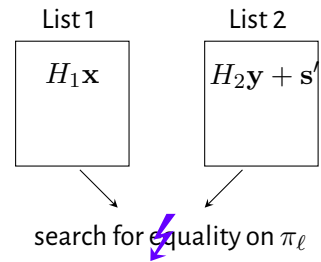
Stern and Dumer

$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$



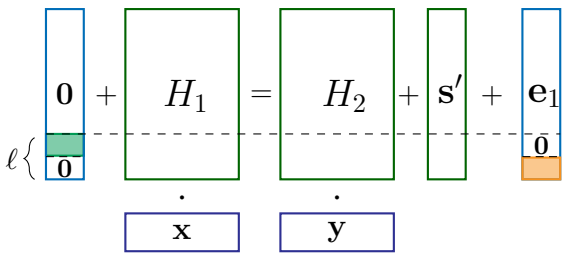
Dumer's Algorithm

$\mathrm{wt}(\pi_\ell(\mathbf{e}_1))$ is small



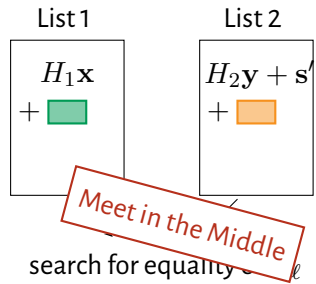
Stern and Dumer

$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$



Dumer's Algorithm

$\mathrm{wt}(\pi_\ell(\mathbf{e}_1))$ is small

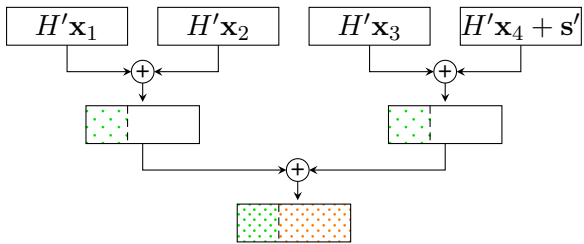


MMT, BJMM, MO and BM

Cryptography Research Centre

$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$

$\mathbf{e}_2$
$=$
$\mathbf{x}_1$
$+$
$\mathbf{x}_2$
$+$
$\mathbf{x}_3$
$+$
$\mathbf{x}_4$



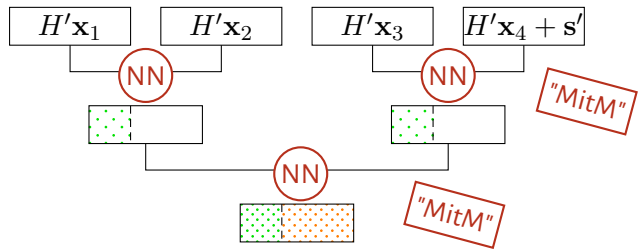
MMT, BJMM, MO and BM

Cryptography Research Centre

$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$

$\mathbf{e}_2$
$=$
$\mathbf{x}_1$
$+$
$\mathbf{x}_2$
$+$
$\mathbf{x}_3$
$+$
$\mathbf{x}_4$

MMT / BJMM Algorithm



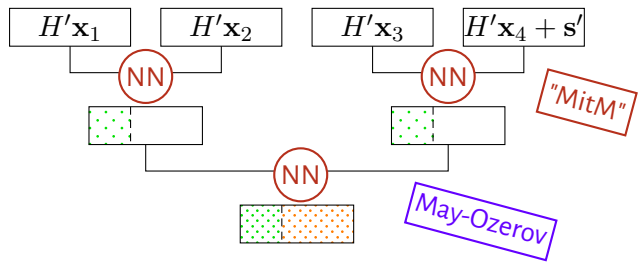
MMT, BJMM, MO and BM

Cryptography Research Centre

$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$

May-Ozerov Algorithm

$\mathbf{e}_2$
$=$
$\mathbf{x}_1$
$+$
$\mathbf{x}_2$
$+$
$\mathbf{x}_3$
$+$
$\mathbf{x}_4$



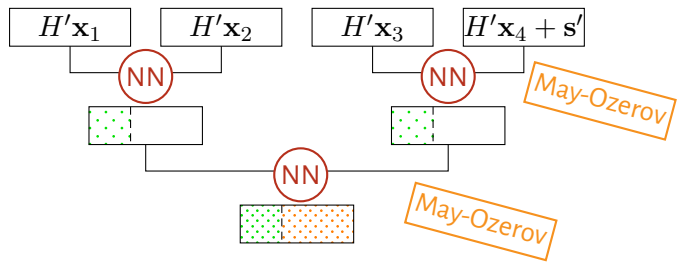
MMT, BJMM, MO and BM

Cryptography Research Centre

$$H'\mathbf{e}_2 = \mathbf{s}' + \mathbf{e}_1$$

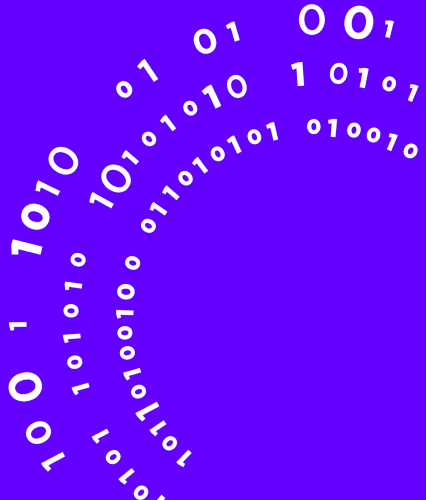
Both-May Algorithm

$\mathbf{e}_2$
$=$
$\mathbf{x}_1$
$+$
$\mathbf{x}_2$
$+$
$\mathbf{x}_3$
$+$
$\mathbf{x}_4$

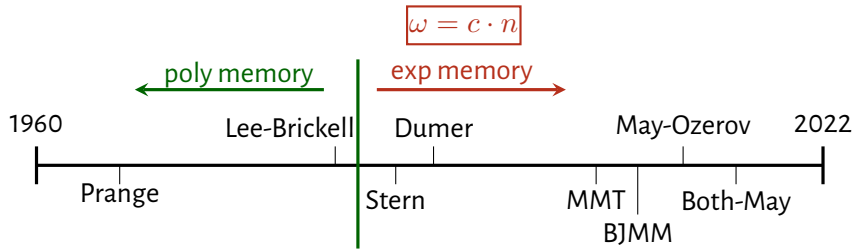


$$T = T_{\text{Perm}} \cdot (T_{\text{Gauss}} + T_{\text{Tree}})$$

Memory Cost



Memory Cost



How to account for memory usage?

conservative: don't

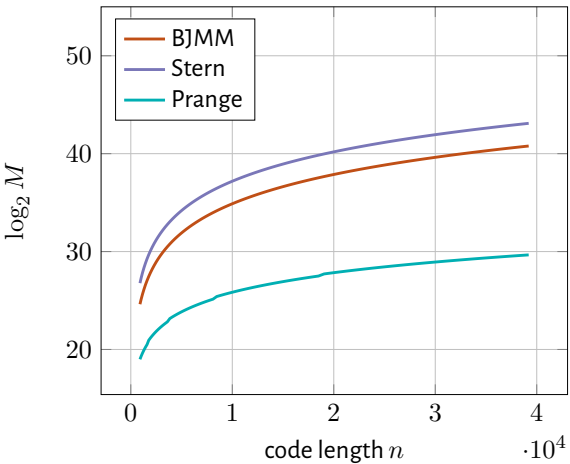
$f(M) = 1$

realistic: time penalty

time T, memory M
$\Rightarrow$ cost $T \cdot f(M)$

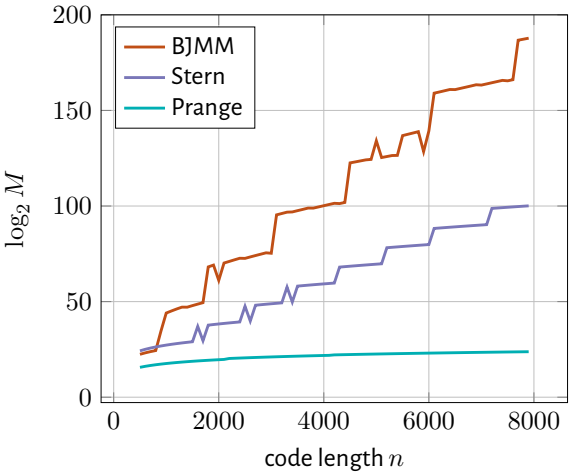
e.g. $f(M) = \log_2 M$
or $f(M) = \sqrt[3]{M}$

BIKE / HQC



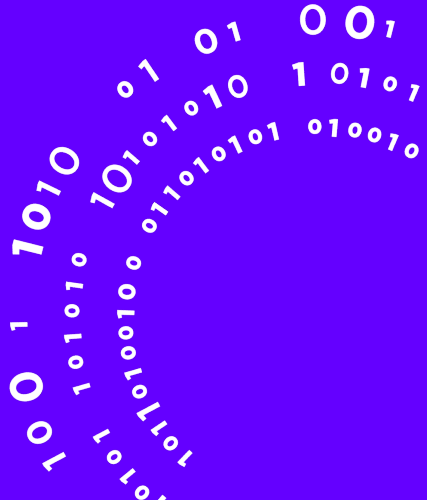
- $\omega = \sqrt{n}$ and $k = \frac{n}{2}$
- low / moderate memory usage

McEliece



- $\omega = \frac{n}{5 \log_2 n}$ and $k = \frac{4n}{5}$
- high memory usage

Security Estimates



BIKE / HQC

Cryptography Research Centre

Memory $< 2^{40}$

very small ω

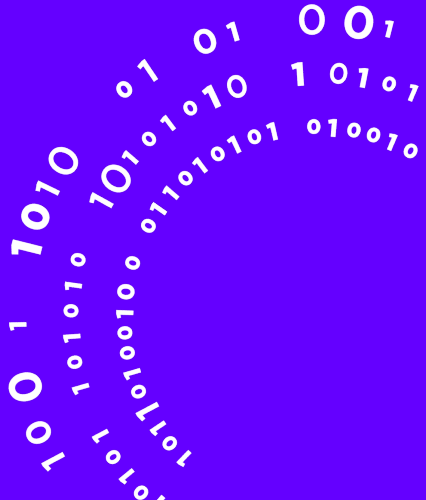
		Category 1 (AES-128)	Category 3 (AES-192)	Category 5 (AES-256)
BIKE	constant access	3	3	4
	$\log M$ access	7	8	10
	$\sqrt[3]{M}$ access	9	10	12
HQC	constant access	3	6	4
	$\log M$ access	7	11	8
	$\sqrt[3]{M}$ access	8	13	10

Classic McEliece

Cryptography Research Centre

	Category 1	Category 3	Category 5a	Category 5b	Category 5c
constant access (Memory: 2^{90} to 2^{200})	− 2	−27	−26	−26	4
$M \leq 2^{80}$	0	−24	−14	−14	21
$M \leq 2^{60}$	2	−20	−10	− 9	26
$\log M$ access	5	−20	−19	−19	11
$\sqrt[3]{M}$ access (Memory: 2^{25} to 2^{47})	13	− 8	3	4	40

Conclusion



Conclusion

Cryptography Research Centre

- BIKE / HQC secure under conservative metrics
- larger $\omega \Rightarrow$ more memory
- memory access cost matters
- Decide for a metric
  (for which? `ia.cr/2021/1634`)

Thank you! **2021/1243**

References I

Aragon, N., Barreto, P., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Gueron, S., Guneysu, T., Melchor, C. A., et al. (2020). BIKE: bit flipping key encapsulation.

Becker, A., Joux, A., May, A., and Meurer, A. (2012). Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 520–536. Springer.

Both, L. and May, A. (2018). Decoding linear codes with high error rate and its impact for lpn security. In *International Conference on Post-Quantum Cryptography*, pages 25–46. Springer.

Chou, T., Cid, C., UiB, S., Gilcher, J., Lange, T., Maram, V., Misoczki, R., Niederhagen, R., Paterson, K. G., Persichetti, E., et al. (2020). Classic McEliece: conservative code-based cryptography 10 october 2020.

Dumer, I. (1991). On minimum distance decoding of linear codes. In *Proc. 5th Joint Soviet-Swedish Int. Workshop Inform. Theory*, pages 50–52.

References II

Esser, A. and Bellini, E. (2021). Syndrome decoding estimator. *Cryptology ePrint Archive*.

Lee, P. J. and Brickell, E. F. (1988). An observation on the security of mceliece's public-key cryptosystem. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 275–280. Springer.

May, A., Meurer, A., and Thomae, E. (2011). Decoding random linear codes in $\tilde{O}(2^{0.054n})$. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 107–124. Springer.

May, A. and Ozerov, I. (2015). On computing nearest neighbors with applications to decoding of binary linear codes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 203–228. Springer.

Melchor, C. A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Persichetti, E., Zémor, G., and Bourges, I. (2020). Hamming quasi-cyclic (HQC).

References III

Prange, E. (1962). The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9.

Stern, J. (1988). A method for finding codewords of small weight. In *International Colloquium on Coding Theory and Applications*, pages 106–113. Springer.


TII
Technology
Innovation
Institute
Cryptography
Research
Centre

tii.ae